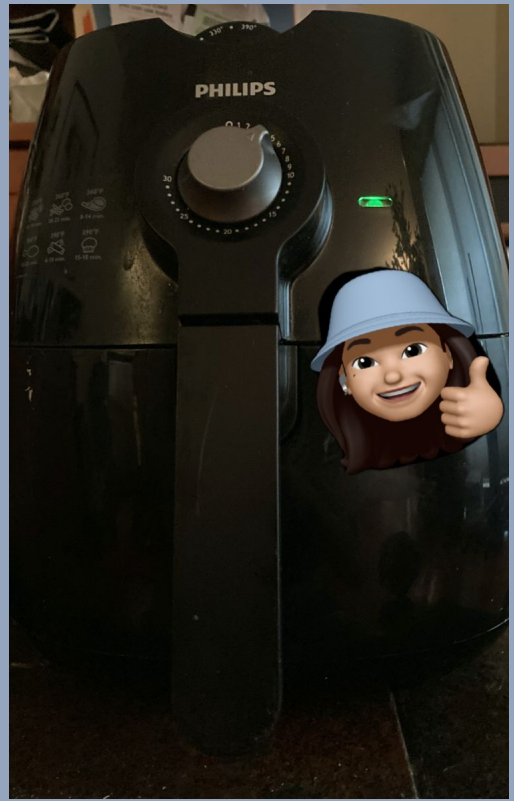


THE AIR FRYERS PRESENT...

ALBERTI CIPHER

Zoe Piccirillo & Kaylee Yin

01

WHAT IS ALBERTI?

A brief introduction

02

HISTORY

Uses throughout the years & variations of the cipher

03

ENCODING/DECODING

How to use the cipher with a walkthrough

04

SECURITY

Pitfalls, comparisons and more secure alternatives

05

OUR CODE

Encoder/decoder for our version & DIY Alberti cipher code

DISCUSSIONS

WHAT IS ALBERTI?

01

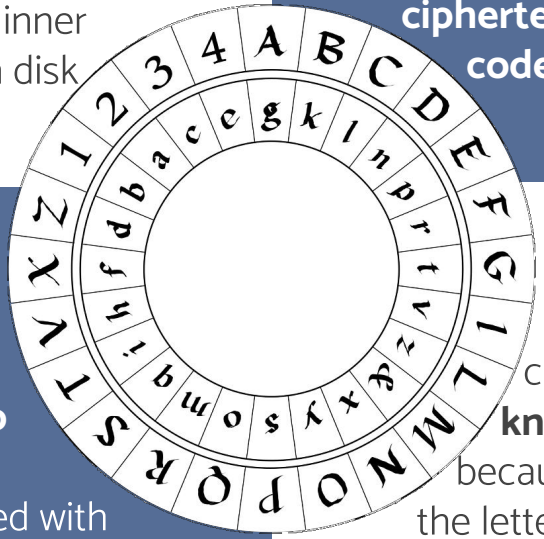
A Polyalphabetic Cipher

The Alberti cipher is the **first instance of a *polyalphabetic cipher***, which are ciphers based on multiple **substitution alphabets**. Created in 1467 by Leon Battista Alberti, the cipher revolutionized encryption in the West. Alberti himself is considered the **father of Western Cryptology**, and his cipher is relatively simple to implement with the assistance of what are known as Alberti's disks. There are multiple variations to this cipher, but we will be focusing on his initial version as he stated in his treatise *De Cifris.*

FUNDAMENTALS

TWO METAL DISCS

The Alberti cipher is best simplified through Alberti's disks, which traditionally consist of **two concentric metal disks** (the inner one mobile and the outer one immobile) attached by a common axle so that the inner disk is able to move. Each disk Is divided into 24 cells.



THE INNER DISK: *CIPHERTEXT*

➤ Contained a **randomized** Latin alphabet **combined with an ampersand.**
➤ Alberti deliberately left out numbers in the inner disc so that **no numbers would appear in the ciphertext, thus concealing the code-numbers.**

THE OUTER DISK: *PLAINTEXT*

➤ Inscribed with letters in the **Latin alphabet: no 'J', 'U', and 'W.'**
➤ **'H', 'K', and 'Y'** replaced with numbers 1 through 4 used in reference to a **codebook containing preselected phrases.**

UNBREAKABLE?

It's impossible to break the cipher **without having prior knowledge of its methods** because frequency distribution of the letters was masked and frequency analysis was of no help. As a result, Alberti is considered more convenient than the Vigenère cipher.

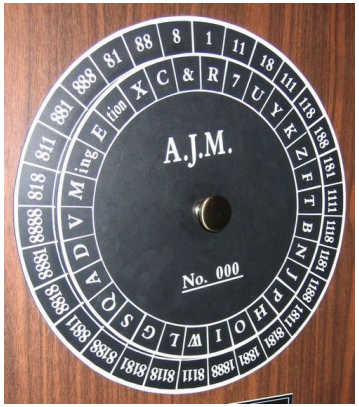
02

HISTORY

TIMELINE

The Jefferson Disk (1795)

→ Axle with 36 wooden disks, each of which is labeled with a number and holds the letters of the Latin alphabet in a random order.
→ Sender sets up the secret key (order of the disks), rotates the disks to align, then rotates the disks by an arbitrary number of steps, giving the ciphertext.

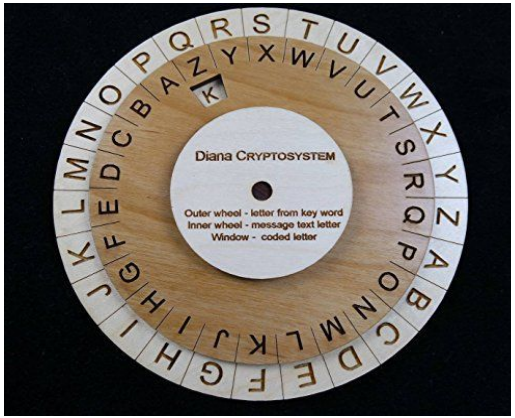


Diana Cipher Disk (1956)

→ Used by US Army Special Forces during the Vietnam War across Vietnam, Cambodia, and Laos.
→ Regular alphabet for both disks.
→ Encrypted messages were sent on high frequency radio channels using morse code, which gave the cipher an extra level of security.

The Union Cipher (1863)

→ Disk used only various numbers of 1 through 8 on its outer ring and a randomly placed alphabet on its movable inner ring.
→ Those exchanging messages each have one of the disks and a prearranged plan to coordinate it with flag or other visual signals.



ENCODING/ DECODING

03

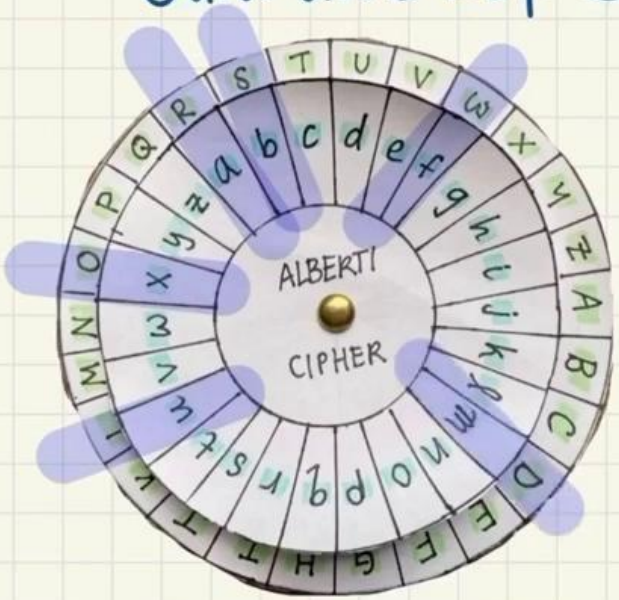
HOW IT WORKS

Each code contains:

- An **outer disk key**, or **base key**
  - This is the letter to which certain letters in the inner disk align when making shifts
- An **inner disk key**
  - This letter in the inner disk **matches up with the outer disk key**
  - A **plaintext letter in the outer disk** becomes the **inner disk ciphertext letter** with which it aligns
- **Disk shifts**
  - The inner key **changes multiple times**, usually in periodic intervals
  - This ensures that **each letter has more than one ciphertext equivalent**

ALBERTI CIPHER

Outer disk key: S Period length: 5 letters



helloworld
0 1 2 3 4 0 1 2 3 4

Shift #1: inner key = M Shift #2 inner key: b

MbyffiBfxau

① Match m with S

② Match b with S

Walkthrough: “helloworld”

04

SECURITY

INNER DISK ISSUES

Universal inner disk = easy to crack

An inner disk using **Alberti's arrangement or the alphabet in order** can easily be cracked

- If you know the arrangement of the inner disk, you simply have to **try every possible outer disk key** and you will decode the message

Solution: _unique_ inner disk for your ciphers

If you create **your own inner disk of characters** that's only known by you and the person with whom you're communicating, **it's much harder to crack**

- You'd have to guess the inner disk AND the outer disk key
- Just by shuffling the alphabet, there are 26! combinations of inner disks: that's roughly **$4.0 * 10^{26}$ possible inner disks!**

05

GITHUB REPO: github.com/zpicci12/alberti_cipher

1
Encoder/Decoder

Encode and decode using an Alberti cipher composed of the **26 letters of the alphabet** (non-traditional) on both disks.

2
DIY Alberti Cipher

Create a **custom inner disk** to make **more secure ciphers**. The outer disk will remain the same (English alphabetic order; A-Z).

THANK YOU!